Foundations of Cryptography - Exercise 4

Alexander Maryanovsky

December 19, 2011

1. (5 points) Let $\{X_n\}_{n\in\mathbb{N}}$ be a Boolean distribution ensemble (i.e. $\mathrm{Supp}(X_n) = \{0,1\}$ for every n), let $\varepsilon : \mathbb{N} \mapsto [0,1]$ and let A be a PPT such that

$$\Pr_{x\leftarrow X_n}[A(1^n) = x] \quad \geq \quad \frac{1}{2} + \varepsilon(n)$$

for every $n \in \mathbb{N}$. Prove that there exists a PPT B such that

$$\Pr_{x\leftarrow X_n}[B(1^n, x) = 1] - \Pr_{x\leftarrow\{0,1\}}[B(1^n, x) = 1] \quad \geq \quad \varepsilon(n)$$

for every $n \in \mathbb{N}$.

2. (5 points) Let $f : \{0,1\}^n \mapsto \{0,1\}^n$ be a one-way function. Prove that for any PPT it holds that

$$\Pr_{x\leftarrow\{0,1\}^n, i\leftarrow[n]}[A(f(x), i) = x[i]] \quad \leq \quad 1 - \frac{1}{2n^2}$$

for large enough $n \in \mathbb{N}$, where $x[i]$ is the ith bit of x.

Solution

1. Let B be the following algorithm:

```
Input: 1^n, x
p←A(1^n)
if (p=x)
  return 1
else
  return 0
```

Clearly B is a PPT and $\Pr[B(1^n, x) = 1] = \Pr[A(1^n) = x]$ for all $n \in \mathbb{N}$ and $x \in \{0,1\}$. It follows that

$$\begin{aligned} \Pr_{x\leftarrow X_n}[B(1^n, x) = 1] - \Pr_{x\leftarrow\{0,1\}}[B(1^n, x) = 1] &= \\ \Pr_{x\leftarrow X_n}[A(1^n) = x] - \Pr_{x\leftarrow\{0,1\}}[A(1^n) = x] &\geq \\ \frac{1}{2} + \varepsilon(n) - \frac{1}{2} &= \varepsilon(n) \end{aligned}$$

(the probability that a random coin flip is equal to anything is always $\frac{1}{2}$). B is therefore a PPT as required. ∎

2. Let us show an even stronger bound on the probability of a PPT to guess a random bit correctly. Specifically, we will show that for any PPT A it holds that

$$\Pr_{x\leftarrow\{0,1\}^n, i\leftarrow[n]}\left[A\left(f\left(x\right),i\right)=x\left[i\right]\right] \quad\leq\quad 1-\frac{c}{n}$$

for any $c<1$.

Let us, therefore, assume, by contradiction, that for some PPT A

$$\Pr_{x\leftarrow\{0,1\}^n, i\leftarrow[n]}\left[A\left(f\left(x\right),i\right)\neq x\left[i\right]\right] \quad<\quad \frac{c}{n}$$

and let B be the following algorithm:

```
Input: y∈ {0,1}^n
for each i from 1 to n
   x[i]←A(y,i)
return x
```

Clearly B is a PPT.

Now, let $W_n\left(x\right)$ be the number of bits that B gets wrong on $f\left(x\right)$, i.e.

$$W_n\left(x\right) \quad=\quad \sum_{i=1}^{n}\mathbb{I}\left[B\left(f\left(x\right)\right)\left[i\right]\neq x\left[i\right]\right]$$

where $\mathbb{I}$ is the indicator (characteristic) function. Clearly $B\left(f\left(x\right)\right)\left[i\right]=A\left(f\left(x\right),i\right)$, and therefore

$$W_n\left(x\right) \quad=\quad \sum_{i=1}^{n}\mathbb{I}\left[A\left(f\left(x\right),i\right)\neq x\left[i\right]\right]$$

We shall now attempt to calculate $\mathrm{E}\left[W_n\left(x\right)\right]$ and then use that to get a lower bound on $\Pr_{x\leftarrow\{0,1\}^n}\left[W_n\left(x\right)<1\right]$ via Markov's inequality.

$$\begin{aligned}
\mathrm{E}\left[W_n\left(x\right)\right] &= \mathrm{E}\left[\sum_{i=1}^{n}\mathbb{I}\left[A\left(f\left(x\right),i\right)\neq x\left[i\right]\right]\right]\\
&= \sum_{i=1}^{n}\mathrm{E}\left[\mathbb{I}\left[A\left(f\left(x\right),i\right)\neq x\left[i\right]\right]\right]\\
&= \sum_{i=1}^{n}\Pr_{x\leftarrow\{0,1\}^n}\left[A\left(f\left(x\right),i\right)\neq x\left[i\right]\right]\\
&= n\cdot\Pr_{x\leftarrow\{0,1\}^n, i\leftarrow[n]}\left[A\left(f\left(x\right),i\right)\neq x\left[i\right]\right]\\
&< n\cdot\frac{c}{n}\\
&= c
\end{aligned}$$

and finally, by Markov's inequality $\Pr_{x\leftarrow\{0,1\}^n}\left[W_n\left(x\right)<1\right]\geq 1-\mathrm{E}\left[W_n\left(x\right)\right]>1-c>0$. In other words, the probability that B gets all of the bits of x correctly is non-negligible, in contradiction to f being a one-way function. We conclude, then, that such an algorithm A does not exist. ■